Утверждаю
Ректор
_____ Л.Н.Горбатова
«26» 05 2021 г.

ПРАВИЛА
работы сотрудников со средствами автоматизации, установленными на рабочих местах в федеральном государственном бюджетном образовательном учреждении высшего образования «Северный государственный медицинский университет» Министерства здравоохранения Российской Федерации

Версия 2.0

Дата введения: 26.05.2021

Архангельск
2021

	Должность	Фамилия/подпись	Дата
Разработал	Директор информационно-интеллектуального центра	Трифонов И.А.	02.04.2021.
Проверил	Начальник управления правового и кадрового обеспечения	Котлов И.А.	02.04.2021.
Согласовал	Первый проректор, проректор по учебно-воспитательной работе	Оправин А.С.	02.04.2021.
	Проректор по цифровой трансформации и инфраструктурному развитию	Халезин А.С.	02.04.2021.

1. Рассмотрено на заседании Ученого совета, протокол № 12 от «14» 04 2021 г.
2. Утверждено и введено в действие приказом Ректора, № 146 от «26» 05 2021 г.
3. Соответствует требованиям СГМУ.
4. Введено в действие взамен правил работы сотрудников со средствами автоматизации, установленными на рабочих местах – версия 1.0.

СОДЕРЖАНИЕ

1.ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящие Правила определяют порядок работы сотрудников ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России (далее Университет) со средствами автоматизации, установленными на рабочих местах.

1.2. Правила подлежат применению во всех подразделениях Университета.

1.3. Целью настоящих Правил является определение порядка работы пользователей, распределение сетевых ресурсов коллективного пользования и поддержание необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации, а также более эффективное использование сетевых ресурсов и уменьшение риска умышленного или неумышленного неправильного их использования.

1.4. Персональные компьютеры (в том числе любая их часть), серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование являются собственностью Университета и предоставляются работникам для осуществления ими своих должностных обязанностей.

1.5. Запрещается производить действия, перечисленные в общем списке нарушений (Приложение 1).

1.6. Персональный компьютер с набором программного обеспечения, установленного в соответствии со стандартом автоматизированных рабочих мест для специалистов Университета, принятым для данного подразделения, и технические средства коммуникации (далее - АРМ) предоставляется сотруднику при приеме на работу в состоянии, пригодном для выполнения должностных обязанностей.

2.ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ - автоматизированное рабочее место;

ОИТ - отдел информационных технологий;

АИБ - Администратор информационной безопасности.

3. ОТВЕТСТВЕННОСТЬ

3.1. Начальник ОИ несет ответственность:

- за организацию надлежащего доведения настоящих

правил до руководителей структурных подразделений Предприятия.

3.2. Сотрудники ОИ несут ответственность:

- за работоспособность информационной системы Университета в целом и каждого АРМ в отдельности;

- за установку и поддержку всех компьютерных систем, функционирующих в Университете;

- за комплектацию персональных компьютеров аппаратными и программными средствами, а также их расположение;

- за контроль над установленным на компьютере программным обеспечением;

- за организацию и обеспечение порядка работы электронной почты.

3.3. Руководители структурных подразделений предприятия несут ответственность:

- за организацию надлежащего доведения и контроль настоящих Правил до сотрудников Университета.

4. ПЕРСОНАЛЬНЫЕ КОМПЬЮТЕРЫ НА РАБОЧИХ МЕСТАХ

4.1. К работе в системе допускаются лица, назначенные на соответствующую должность, прошедшие инструктаж у руководителя подразделения, АИБ и регистрацию в ОИ.

4.2. Каждый сотрудник Университета, обеспеченный персональным компьютером, получает:

- персональное сетевое имя,
- пароль,
- адрес внутренней электронной почты.

4.3. Все автоматизированные рабочие места, установленные в Университете, имеют унифицированный набор офисных программ, предназначенных для получения, обработки и обмена информацией, определенный стандартом автоматизированных рабочих мест для специалистов Университета.

4.4. Унификация программных и аппаратных средств является основополагающей стратегией автоматизации, предназначенной для исключения возможных случаев несовместимости типов данных и видов аппаратных средств. Изменение установленной конфигурации возможно по служебной записке, согласованной с начальником ОИ.

4.5. Перемещение любых средств вычислительной техники производится в соответствии со служебной запиской, начальнику ОИ не менее, чем за сутки и подписанной руководителем структурного подразделения.

4.6. Самовольное перемещение компьютеров, принтеров и т.д. является нарушением персональной ответственности за сохранность переданных сотруднику во временное пользование средств автоматизации.

4.7. Самостоятельная установка программного обеспечения на АРМ запрещена.

4.8. Установка и удаление любого программного обеспечения производится только сотрудниками ОИ, установка любых программ производится на

основании заявки, согласованной с руководителем подразделения, в котором работает сотрудник.

4.9. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться в ОИ.

4.10. ОИ обязан принимать меры по ограничению возможностей несанкционированной установки программ (включая отключение дисководов, CD/DVD-приводов и USB-портов у пользователей, которые не должны по своим служебным обязанностям обмениваться информацией на внешних носителях вне Университета).

4.11. Передача электронных документов внутри Университета производится только посредством общих папок соответствующих отделов, а также средствами электронной почты, без участия физических магнитных носителей.

5. РЕСУРСЫ ЛОКАЛЬНОЙ СЕТИ

5.1. Для успешного выполнения своих служебных обязанностей каждый сотрудник обеспечивается доступом к соответствующим информационным ресурсам.

5.2. Информационными ресурсами являются каталоги и файлы, хранящиеся на дисках серверов Университета, базы данных, электронная почта (включая каталоги электронной почты), internet-серверы (внутри Университета и за его пределами).

5.3. Для доступа к информационным ресурсам пользователю присваивается уникальное сетевое имя и буквенно-цифровой пароль длиной не менее 6 знаков. Информация о реквизитах доступа пользователя к информационным ресурсам является конфиденциальной и не подлежит разглашению. Пользователь обязан хранить в секрете, присвоенные ему

аутентификационные данные. Ни при каких условиях пароль не может быть сообщён другому лицу.

5.4. Во избежание получения несанкционированного доступа к ресурсам автоматизированного рабочего места сотрудника устанавливается хранитель экрана (Screensaver), который автоматически включается через 10 минут отсутствия работы на данном компьютере, при этом выход из режима хранителя экрана возможен только при введении аутентификационных данных пользователя.

5.5. При необходимости отлучиться от рабочего места пользователь обязан принудительно запустить хранитель экрана, или использовать Блокировку средствами ОС.

5.6. Основными рабочими каталогами являются личные каталоги сотрудников и каталоги подразделений, созданные в соответствии с особенностями их работы.

5.7. Доступ сотрудников к ресурсам сети осуществляется согласно матрицы доступа.

5.8. Временное расширение прав доступа осуществляется ОИ согласно служебной записки завизированной руководителем подразделения сотрудника, которому необходимо предоставить доступ.

6. РАБОТА В ГЛОБАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ INTERNET

6.1. Информационная система Университета имеет выход в internet. В соответствии со служебными обязанностями сотрудникам может предоставляться доступ к сети internet для получения оперативной и достоверной информации в области профессиональной деятельности.

6.2. Разрешение и изменение доступа к ресурсам internet (в том числе к внешним почтовым сервисам) производится на основании заявки. Пользователь имеет право использовать в работе предоставленные ему

сетевые ресурсы в оговоренных в настоящей инструкции рамках, если иное не предусмотрено отдельным распоряжением.

6.3. В целях обеспечения информационной безопасности, АИБ Университета вправе ограничивать доступ к некоторым сетевым ресурсам (потенциально опасные ресурсы, ресурсы развлекательного характера, файлообменные сети и прочее) вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов.

6.4. Пользователям необходимо принимать во внимание, что internet-канал является потенциальным путем вторжения в локальную компьютерную сеть. Следует воздерживаться от заполнения информационных форм, в которых требуется сообщать о структуре сети, названии серверов, реквизитов доступа в сеть, параметров IP-протокола и персональных сетевых настройках.

6.5. Любые файлы, принятые от internet-серверов, следует проверять программой-антивирусом.

6.6. По использованию internet ведется аудит, и его результаты поступают в архив Университета.

6.7. Действия любого пользователя могут быть запротоколированы, и использоваться для принятия решения о применении к нему санкций. Сотрудникам, имеющим право доступа к ресурсам internet, запрещено передавать или загружать на компьютер материал, не относящийся к его профессиональной деятельности.

7.ЭЛЕКТРОННАЯ ПОЧТА

7.1. При работе с корпоративной электронной почтой пользователь должен учитывать следующие принципиальные положения:

- электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;
- электронная почта не является средством передачи информации, обеспечивающим конфиденциальность передаваемой информации. Передачу конфиденциальной информации вне локальной сети необходимо осуществлять только в зашифрованном виде;
- электронная почта не является средством передачи информации, гарантированно идентифицирующим отправителя сообщения.

7.2. Каждый сотрудник (при наличии служебной необходимости в электронной почте) получает почтовый адрес вида (фамилия)@nsmu.ru в домене Университета.

7.3. Адрес электронной почты выдается сотрудником ОИ при начальной регистрации пользователя в домене или на основании заявки.

7.4. В случае острой необходимости (начало нового проекта, необходимость группового адреса или др.) возможно создание дополнительного электронного адреса с переадресацией сообщений с этого адреса указанным сотрудникам.

7.5. Дополнительный адрес выдается по служебной записке руководителя структурного подразделения начальнику ОИ.

7.6. Размер почтового ящика пользователя не ограничен, однако письма со сроком давности не менее 6 месяцев следует удалять, если в них нет необходимости.

7.7. Электронная почта Университета является средством коммуникации, распределения информации и управления процессами в производственных целях: повышения эффективности труда сотрудников и экономии ее ресурсов.

7.8. Корпоративная электронная почта Университета предназначена исключительно для использования в служебных целях.

7.9. Функционирование электронной почты обеспечивается оборудованием, каналами связи и иными ресурсами, принадлежащими Университету.

7.10. Все почтовые сообщения, переданные или принятые с использованием корпоративной электронной почты, принадлежат Университету и являются неотъемлемой частью ее производственного процесса.

7.11. Любые сообщения корпоративной электронной почты могут быть прочитаны и использованы в интересах Университета либо удалены сотрудниками ОИ Университета.

7.12. В связи с п.9.7, п.9.8, п.9.10 и п.9.11, а также в целях соблюдения законодательства Российской Федерации о тайне переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан, пользователям корпоративной электронной почты Университета запрещено вести частную переписку с использованием средств корпоративной электронной почты.

7.12.1. К частной переписке относится переписка, не связанная с исполнением сотрудником своих должностных обязанностей.

7.12.2. Использование корпоративной электронной почты Университета для частной переписки сотрудником, надлежащим образом, ознакомленным с данными Правилами, является нарушением трудовой дисциплины.

7.13. Подписываясь в Листе ознакомления Правил, сотрудник дает согласие на ознакомление и иное использование в интересах Университета его переписки, осуществляемой с использованием корпоративной электронной почты, и соглашается с тем, что любое использование его переписки, осуществляемой с использованием корпоративной электронной почты, не может рассматриваться как нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан.

7.14. Использование сообщений корпоративной электронной почты осуществляется уполномоченными сотрудниками Университета в соответствии с их функциями, определенными в данных Правилах и в иных локальных нормативных актах Университета.

7.15. Просмотр и иное использование электронных сообщений в интересах Университета осуществляется сотрудниками Университета в целях обеспечения защиты конфиденциальных сведений, обеспечения нормальной работоспособности системы электронной почты, в рамках обслуживания сервисов электронной почты, при выполнении ручной пересылки сообщений, приходящих на корпоративные электронные адреса сотрудникам или группам сотрудников, а также по мотивированным запросам прямых или непосредственных руководителей любых сотрудников, чью почту необходимо использовать в интересах Университета..

7.16. Запрещается использование сотрудниками своего электронного адреса для подписки на рассылки и другие сервисы Интернет, а также при регистрации на любых сайтах Интернет, если они прямо не связаны с должностными обязанностями в Университете.

7.17. Все исходящие и входящие сообщения корпоративной электронной почты должны храниться на центральном почтовом сервере Университета не менее 6 месяцев в виде, доступном для просмотра, пересылки и иного использования.

7.18. Исходящие электронные сообщения сотрудников Университета должны содержать подпись сотрудника в формате по форме Приложения 2.

7.19. Время доставки электронного сообщения составляет в среднем от нескольких минут до нескольких часов. В случае невозможности доставки сообщения адресату почтовые сервера направляют отправителю служебное сообщение с указанием причин невозможности доставки. Время доставки

такого сообщения может достигать суток с момента отправки сообщения адресату.

7.20. В случае получения служебного сообщения о невозможности доставки сообщения адресату или получения извещения от адресата о том, что он не получил отправленное ему сообщение, необходимо связаться с сотрудником ОИ, но ни в коем случае не отправлять письмо или несколько писем повторно.

7.21. Отказ от дальнейшего предоставления сотруднику сервисов корпоративной электронной почты может быть вызван нарушениями, определенными в пунктах 9.8, 9.11, 9.12, 9.13, 9.20, 9.22, Приложения 1 к настоящим Правилам.

7.22. Прекращение предоставления сотруднику услуг корпоративной электронной почты наступает при прекращении действия трудового договора сотрудника.

8. ПОРЯДОК УСТАНОВКИ - СНЯТИЯ РАБОЧИХ МЕСТ ПРИ ПРИЕМЕ - УВОЛЬНЕНИИ СОТРУДНИКОВ

8.1. При возникновении какой-либо вакансии в структурном подразделении, его руководитель сообщает об этом работнику отдела кадров. При необходимости организации нового рабочего места следует информировать начальника ОИ за 2 недели до предполагаемого выхода сотрудника на работу. Заявка подается в бумажном виде начальнику ОИ и дублируется в электронном виде. В заявке следует указать расположение рабочего места, фамилию, имя и отчество сотрудника, его должность, примерный круг обязанностей, дату первого рабочего дня и особые требования к АРМ, если такие имеются. ОИ обязуется, при технической возможности, устанавливать рабочие места раньше оговоренного срока. При возникновении производственной необходимости установки дополнительного аппаратного обеспечения, руководителю подразделения следует направить

соответствующую заявку начальнику ОИ. При наличии данного аппаратного средства в резерве, установка производится в течении 5 дней с момента получения заявки. В случае необходимости заказа оборудования, представители ОИ извещают о примерных сроках выполнения заявки. На все обращения по электронной почте в ОИ сотрудники ОИ обязаны отвечать в течении 2 рабочих дней.

8.2. Решение об увольнении сотрудника обязательно должно доводиться до начальника ОИ немедленно, по принятию решения, руководителем подразделения, в котором работает увольняемый сотрудник. Это необходимо для своевременной блокировки учетной записи, архивирования данных и перевода АРМ в резерв. В письме следует сообщить фамилию сотрудника, которому передаются дела увольняющегося для того, чтобы начальник ОИ мог своевременно перевести ресурсы увольняемого на сотрудника, принимающего дела. В этом случае все документы и ресурсы переходят другому сотруднику. По просьбе руководителя подразделения АРМ уволенного сотрудника может не демонтироваться, при условии, что вновь принятый сотрудник начнет работать не позже, чем через 3 недели. В случае сокращения должности после увольнения сотрудника производится расформирование рабочего места и перевод техники в резерв.

9. ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

9.1. Требования безопасности во время работы. Пользователь во время работы обязан:

- содержать в порядке и чистоте рабочее место;
- выполнять санитарные нормы и соблюдать режимы работы и отдыха;
- соблюдать правила эксплуатации вычислительной техники в соответствии с правилами по работе с АРМ;
- во время перерывов с целью снижения нервно-эмоционального напряжения, утомления зрительного анализатора целесообразно выполнять комплексы упражнений.

9.2. При работе запрещается:

- трогать кабели и провода, соединяющие блоки ПЭВМ, перемещать устройства, находящиеся под напряжением;
- оставлять без присмотра включенные ПЭВМ и отдельные устройства более 3х часов, если иное не предусмотрено;
- производить самостоятельно любые виды ремонта и устранение неисправностей.

9.3. Требования безопасности в аварийной ситуации Действия в случае аварийной ситуации:

- при нарушении работы ПЭВМ, перегорании предохранителей и т.п. аппаратура должна быть немедленно отключена;
- при временном отключении электроэнергии тумблера электропитания должны быть выключены;
- при появлении запаха гари, дыма в помещении или на рабочем месте сеть электропитания ПЭВМ и других устройств должна быть выключена и приняты меры к обнаружению источника загорания и тушению имеющимися

средствами пожаротушения (углекислотные огнетушители, асбестовые покрывало, песок);

- при обнаружении пожара или признаков возгорания пользователь должен немедленно сообщить об этом в службу пожарной охраны.

9.4. Требования безопасности по окончанию работы

По окончанию работы пользователь должен:

- отключить ПЭВМ от сети;
- привести в порядок рабочее место.

Приложение 1 к Положению(рекомендуемое)

Общий список нарушений

1. Самовольное вскрытие компьютеров, сетевого и периферийного оборудования;
2. Хранение важной информации в незащищенном от сбоя хранилище на локальном компьютере.
3. Подключение к компьютеру дополнительного оборудования без санкции сотрудников ОИ, изменение настройки BIOS, а также загрузка автоматизированных рабочих мест с дискет и других внешних носителей информации;
4. Самовольный вынос компьютерного оборудования с территории;
5. Самостоятельная установка или удаление установленных программ на автоматизированных рабочих местах, изменение настроек операционной системы и приложений, влияющих на работу сетевого оборудования и сетевых ресурсов;
6. Использование чужих учётных данных в локальной сети;
7. Передача личных реквизитов доступа кому-либо;

8. Небрежное использование компьютерного оборудования, приведшее к его выходу из строя;

9. Использование программ, не предназначенных для выполнения прямых служебных обязанностей;

10. Повреждение, уничтожение или фальсификация информации, не принадлежащей данному пользователю;

11. Рассылка сотрудником с корпоративного электронного адреса не заказанной получателем корреспонденции рекламного характера (спама);

12. Рассылка корреспонденции, содержащей вредоносные программы компьютерные вирусы, троянские программы и т.п.;

13. Нарушение порядка обращения с конфиденциальной информацией;

14. Рассылка корреспонденции оскорбительного или противозаконного характера;

15. Нарушение правил пользования информационными системами, повлекшее потерю (повреждение) данных или разглашение конфиденциальных сведений;

16. Систематический доступ к ресурсам internet, не входящим в служебные обязанности и сферу профессиональных интересов;

17. Несанкционированное использование внешних почтовых сервисов;

18. Пересылка или получение из internet больших файлов, а также изображений, не связанных с профессиональной деятельностью;

19. Подписка на развлекательные телеконференции и списки рассылки;

20. Использование компьютерных ресурсов в личных целях или во вред Университету;

21. Обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация;

22. Любые действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и серверов сети Университета, равно как и любых других компьютеров в internet;

23. Систематическое (то есть неоднократное после более, чем двух, официальных предупреждений со стороны ОИ о недопустимости подобных действий) использование корпоративной электронной почты в целях, не связанных с деятельностью компании, с использованием существенных ресурсов почтовых сервисов (обмена медиа-файлами и графикой больших объемов; ведения собственного бизнеса с использованием почтовых ресурсов Университета и т.д.);

24. Иные действия, систематически нарушающие настоящие Правила

Приложение 2 к Положению(рекомендуемое)

Фамилия имя отчество

Служебный телефон:8 (8182) 25 25 25

e-mail: fio@nsmu.ru

Данное сообщение передано с использованием корпоративной электронной почты, принадлежащей ФГБОУ ВПО СГМУ (г. Архангельск) Минздрава России и не предназначенной для ведения частной переписки граждан.

Данное сообщение (включая любые приложения к нему) содержит конфиденциальную информацию, предназначенную исключительно для определенного лица и защищается законодательством. В случае, если Вы не являетесь лицом, которому предназначалась указанная информация, удалите настоящее сообщение. Настоящим Вам также сообщается, что любое несанкционированное раскрытие, копирование или распространение настоящего сообщения или совершение каких-либо действий, основанных на информации, содержащейся в нем, строго запрещено.